CLAIMS

1. User authentication method based on the use of identification biometric techniques comprising an enrolment step (20) and a verification step (40), said enrolment step (20) including the steps of:

- generating (22, 23) a reference biometric template from a first biometric image of a user to be authenticated;

- splitting (25) said reference biometric template into a first and a second reference biometric template portion;

- enciphering (27, 28) said first and second reference biometric template portion; and

- storing (29, 30, 31) each one of said reference biometric template portions into a different memory.

2. Method according to Claim 1, characterised in that said step of storing each one of said reference biometric template portions into a different memory comprises the step of:

- transmitting (29) said first reference biometric template portion from a first system (2) to a device (4), said first system (2) operating in said enrolment step (20);

- storing (30) said first reference biometric template portion into a memory (6) of said device (4), said device (4) operating in said verification step (40);

- transmitting (31) said second reference biometric template portion from said first system (2) to a second system (3), said second system (3) operating in said verification step (40); and

- storing (31) said second reference biometric template portion into a memory (11a) of said second system (3).

3. Method according to any one of Claims 1 or 2, characterised in that said verification step (40) comprises the steps of:

- generating (41, 42) a live template from a second biometric image of said user to be authenticated;
- enciphering (43) said live template; and
- transmitting (44) said live template and said second reference biometric template portion to said device (4).

4. Method according to Claim 3, characterised in that said verification step (40) comprises the steps of:

- deciphering (45, 47) said live template and said second reference biometric template portion;
- recomposing (46) said reference biometric template from said first and second reference biometric template portion; and
- comparing (48) said recomposed reference biometric template with said live template.

5. Method according to Claim 4, characterised in that said verification step (40) comprises the steps of:

- sending (49) a result of said comparison to said second system (3); and
- authenticating (50) or not authenticating said user depending on said result.

6. Method according to any one of Claims 2-5, characterised in that said step of splitting said

reference biometric template into a first and a second reference biometric template portion comprises the step of:

- destroying said biometric template performed by said first system (2).

7. Method according to any one of Claims 2-6, characterised in that said step of enciphering (27, 28) said first and second reference biometric template portion comprises the steps of:

- storing (21) a first and a second key (KE_{pub}, KE_{pr}) and a related digital certificate (C_E) into a memory (7a) of said first system (2), said first and second keys (KE_{pub}, KE_{pr}) being respectively a public key (KE_{pub}) and a private key (KE_{pr}) associated with said first system (2);

- storing (21) a first and a second key (KU_{pub}, KU_{pr}) and a related digital certificate (C_u) into said memory (6) of said device (4), said first and second keys (KU_{pub}, KU_{pr}) being respectively a public key (KU_{pub}) and a private key (KU_{pr}) associated with said user to be authenticated;

- signing (27) said first and second reference biometric template portion with said private key (KE_{pr}) of said first system (2); and

- enciphering (28) said first and second reference biometric template portion with said public key (KU_{pub}) of said user to be authenticated.

8. Method according to any one of Claims 3-7, characterised in that said step of transmitting said live template and said second reference biometric template portion to said device (4) comprises the steps of:

- generating an aleatory value associated with the current data verification step (40), said aleatory value guaranteeing the authenticity of said current data verification step (40);

- signing and enciphering said aleatory value; and

- transmitting said aleatory value to said device (4).

9. Method according to Claims 7 or 8, characterised in that said step of enciphering said comparison biometric template comprises the steps of:

- storing a first and a second key (KV_{pub}, KV_{pr}) and a related digital certificate (C_V) into said memory (11a) of said second system (3), said first and second keys (KV_{pub}, KV_{pr}) being respectively a public key (KV_{pub}) and a private key (KV_{pr}) associated with said second system (3);

- signing (43) said live template with said private key (KV_{pr}) of said second system (3); and

- enciphering (43) said live template with said public key (KU_{pub}) of said user to be authenticated.

10. Method according to any one of Claims 8 or 9, characterised in that said step of deciphering said live template and said second reference biometric template portion comprises the steps of:

- deciphering the signature and the validity of said aleatory value;

- deciphering (45) said second reference biometric template portion with said private key (KU_{pr}) of said user to be authenticated;

- verification its signature (45)

- deciphering (47) said live template with said private key (KU_{pr}) of said user to be authenticated; and

- verification its signature (47).

11. Method according to any one of Claims 5-10, characterised in that said step of sending a result of said comparison to said second device (11) comprises the steps of:

- generating a message containing said result;
- enciphering said message.

12. Method according to any one of the previous claims, characterised in that said identification biometric techniques comprise at least one biometric identification technique of the type selected among: face recognition, fingerprints, hand prints, voice templates, retinal images, calligraphic samples.

13. Method according to any one of Claims 2-12, characterised in that said first and second system (2), (3) are respectively a data enrolment system and a data verification system and said device (4) is a data carrier.

14. Method according to Claim 1, characterised in that said step of splitting said reference biometric template includes the steps of

- splitting said reference biometric template into a plurality of reference biometric template portions, at least some of said reference biometric template portions being used to recompose said reference biometric template.

15. User authentication architecture bases on the use of biometric identification techniques comprising:

- at least one data enrolment system (2) for generating a reference biometric template from a first biometric image of a user to be authenticated, said data enrolment system (2) comprising a Host Computer

(7) to split said reference biometric template into a first and a second reference biometric template portion and for enciphering said first and second reference biometric template portion;

- at least one portable data carrier (4) associated with said user to be authenticated, said data carrier (4) comprising a memory (6a) for storing said first signed and enciphered reference biometric template portion; and

- at least one data verification system (3) comprising a memory (11a) for storing said second signed and enciphered reference biometric template portion.

16. Architecture according to Claim 15, characterised in that said data carrier (4) comprises a microprocessor (5) including a processing logic (5a) for deciphering said first and second reference biometric template portion, verification the signature and recomposing said reference biometric template from said first and second deciphered reference biometric template portion.

17. Architecture according to Claim 16, characterised in that said microprocessor (5) comprises a comparing logic (5b) to compare said recomposed reference biometric template with a live template generated by a second biometric image of the user to be authenticated, said second biometric image of the user to be authenticated being generated by the data verification system (3).

18. Portable data carrier (4) associated with a user that has to be authenticated through a user authentication architecture (1), said data carrier (4)

including a microprocessor (5) comprising a memory (6) for storing a first reference biometric template portion associated with said user to be authenticated, said first reference biometric template portion being signed and enciphered, said portable data carrier being adapted to receive as input, from said user authentication architecture, a second reference biometric template portion and a live template associated with said user to be authenticated, said second reference biometric template portion and said live template being signed and enciphered, said microprocessor (5) further comprising:

- a processing logic (5a) for deciphering said first and second reference biometric template portions and for recomposing therefrom said reference biometric template associated with said user to be authenticated;
- a comparing logic (5b) for comparing said reference biometric template recomposed with said live template and sending a result of said comparison to said user authentication architecture (1).

19. Data carrier according to Claim 18, characterised in that it comprises a substrate whose sizes are substantially rectangular.

20. Data carrier according to any one of Claims 18 or 19, characterised in that said data carrier (4) is an access card or a credit card or a debit card or an identification card or a smart card or a SIM card.

21. Data verification system (3) comprising an electronic device (11) and a portable data carrier (4) associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a

user to be authenticated, said first reference biometric template portion being signed and enciphered;

said electronic device comprising:

- a memory (11a) adapted to store a second reference biometric template portion associated with a user to be authenticated, complementary to said first portion, said second reference biometric template portion being signed and enciphered;

- an image acquiring and processing device (12) for generating a live template;

said electronic device (11) being adapted to encipher and sign said live template, transmitting said second reference biometric template portion and said live template to said portable data carrier (4) and authenticating said user depending on the result of a comparison performed by said data carrier (4) between said live template and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first and second reference biometric template portion.22. Data verification system (3) comprising an electronic device (11) and a portable data carrier (4) associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and enciphered;

said electronic device comprising:

- a first memory (11a, 15) adapted to store a second reference biometric template portion associated with a user to be authenticated, said second reference biometric template portion being signed and enciphered;

- at least a second memory (11a, 15, 3b) adapted to store at least a third reference biometric template portion associated with a user to be authenticated, said third reference biometric template portion being signed and enciphered, wherein said first, second and at least third reference biometric template portions are such that the reference biometric template can be recomposed from a subset of at least two of said reference biometric template portions;

- an image acquiring and processing device (12) for generating a live template;

said electronic device (11) being adapted to encipher and sign said live template, transmitting said second reference biometric template portion and said live template to said portable data carrier (4) and authenticating said user depending on the result of a comparison performed by said data carrier (4) between said live template and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first and second reference biometric template portion.

23. Program for electronic processor that can be loaded into the memory of at least one electronic processor and including program codes for performing the steps of the method according to any one of Claims 1-14 when said program is executed by said electronic processor.